



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,505	01/09/2002	Gary J. Cross	AUS920010952US1	6747
35525	7590	11/15/2006	EXAMINER	
IBM CORP (YA) C/O YEE & ASSOCIATES PC P.O. BOX 802333 DALLAS, TX 75380			HOFFMAN, BRANDON S	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 11/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**MAILED**

**NOV 15 2006**

**Technology Center 2100**

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 10/042,505  
Filing Date: January 09, 2002  
Appellant(s): CROSS, GARY J.

Theodore Fay III (Reg. No. 48,504)  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed August 28, 2006 appealing from the Office action mailed April 12, 2006.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

No amendment after final has been filed.

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

5915021	Herlin et al.	6-1999
5305384	Ashby et al.	4-1994

### **(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

#### ***Claim Rejections - 35 USC § 103***

Claims 1-7, 9-17, 19-27, 29, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baugh et al. (U.S. Patent No. 5,815,553) in view of Herlin et al. (U.S. Patent No. 5,915,021), and further in view of Ashby et al. (U.S. Patent No. 5,305,384).

Regarding claims 1, 11 and 21, Baugh et al. discloses a method/system/computer program product for securing radio transmissions utilizing a conventional radio, said method comprising the steps of:

- Providing a conventional radio, said conventional radio being incapable of encrypting or decrypting signals, said radio including a conventional microphone port that is configured to be coupled to a conventional microphone and a conventional speaker port that is configured to be coupled to a conventional speaker, said radio remaining unmodified (abstract, col. 2, lines 58-62 and fig. 1, ref. num 50, 58, and 62);
- Receiving, within said computer system, an input analog signal from said microphone (col. 2, lines 58-62);

Art Unit: 2136

- Encrypting, within said computer system, said input analog signal utilizing public key encryption to form an encrypted voice file (col. 8, lines 44-47); and
- Passing said encrypted voice file from said computer system to said microphone port that is included within said unmodified radio and transmitting said encrypted voice file utilizing said unmodified radio, wherein radio transmissions from said radio are secured (col. 3, lines 9-14 and fig. 1, ref. num 70 and 74).

Baugh et al. does not specifically teach the input signal is encrypted using public key techniques.

Herlin et al. teaches a method for sending a secure message in a telecommunications system using public key encryption (col. 5, lines 12-35 and col. 9, lines 56-58).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a public key encryption system, as taught by Herlin et al., with the method/system/computer program product of Baugh et al. It would have been obvious for such modifications because the system gains the advantage of securing the recorded message from unauthorized disclosure by an eavesdropper who is monitoring the communication link. By using public key encryption, the recorded message can only be decrypted by the private key that corresponds to the public key used to encrypt the message (see col. 3, lines 60-67 of Herlin et al.).

The combination of Baugh et al. as modified by Herlin et al. do not specifically teach providing a computer system being separate and apart from said radio.

Ashby et al. teaches providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system, said computer system being separate and apart from said radio (fig. 1, ref. num 12, separate from the other components).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine connecting a radio output to a computer input, as taught by Ashby et al., with the method/system/computer program product of Baugh et al./Herlin et al. It would have been obvious for such modifications because encrypting communications from a radio, who is directly connected to a computing device, prevents eavesdropping on police and military communications by encrypting the data directly from the radio (see abstract and col. 1, lines 18-23 of Ashby et al.).

Regarding claims 2, 12 and 22, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the step of encrypting, within said computer system, said input analog signal utilizing a key pair, said key pair including a public key and a private key (see col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 3, 13 and 23, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the step of encrypting, within said computer system, said input analog signal utilizing said public key (see col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 4, 14 and 24, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches wherein the receiving step comprises receiving, within a first application executing within said computer system, said input analog signal from said microphone; wherein the encrypting step comprises encrypting, utilizing said first application, said input analog signal utilizing public key encryption to form said encrypted voice file; wherein the passing step comprises passing said encrypted voice file from said first application to said microphone port of said unmodified radio (see col. 2, lines 58-62, fig. 1, ref. num 50, 58, and 62, col. 3, lines 9-14, fig. 1, ref. num 70 and 74, and col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 5, 15 and 25, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches wherein the receiving step comprises:

- Converting, by a microphone driver that is executing within said computer system, said input analog signal to a file, said file being in a standard voice file format; constantly monitoring, by said first application, inputs received from said microphone; detecting, by said first application, a receipt of said file (see col. 2, line 63 through col. 3, line 25 of Baugh et al.); and

- Wherein the encryption step comprises in response to a detection by said first application of said receipt of said file, encrypting to form said encrypted voice file, by said first application utilizing a public key that is part of a public key/private key pair assigned to said computer system (see col. 2, lines 58-62, fig. 1, ref. num 50, 58, and 62, col. 3, lines 9-14, fig. 1, ref. num 70 and 74, and col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 6, 16 and 26, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the steps of:

- Providing a second conventional radio, said second conventional radio being incapable of encrypting or decrypting signals, said second radio including a second microphone port that is configured to be coupled to a second conventional microphone and a second speaker port that is configured to be coupled to a second conventional speaker, said second radio remaining unmodified (see fig. 1, ref. num 54, 98, and 102 of Baugh et al.);
- Providing a second computer system coupled between said second speaker and said second unmodified radio, wherein outputs from said second radio are received first by said second computer system before being output to said second speaker, said second computer system being separate and apart from said second radio (see fig. 1, ref. num 12, separate from the other components of Ashby et al.);



- Receiving, within said second computer system, an encrypted output from said second speaker port included within said unmodified second radio (see fig. 1, ref. num 86 of Baugh et al.); and
- Decrypting, within said second computer system, said encrypted output utilizing public key encryption to form a decrypted output and outputting said decrypted output from said second computer system to said second speaker (see col. 8, lines 44-47 of Baugh et al.).

Regarding claims 7, 17 and 27, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches wherein within said second computer system the step of receiving further comprises:

- Constantly monitoring, by a second application that is executing within said second computer system, said second speaker port (see col. 3, lines 32-42 of Baugh et al.); and
- Receiving, by said second application, said encrypted output from said second speaker port (see fig. 1, ref. num 86 of Baugh et al.);
- Wherein the decrypting step comprises decrypting, by said second application, said encrypted output utilizing public key encryption (see col. 8, lines 44-47 of Baugh et al.).

Regarding claims 9, 19 and 29, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the steps of obtaining, by said

second computer system, a private key of said computer system; and wherein the decrypting step further comprises decrypting said encrypted output utilizing said private key (see col. 2, lines 58-62, fig. 1, ref. num 50, 58, and 62, col. 3, lines 9-14, fig. 1, ref. num 70 and 74, and col. 8, lines 44-47 of Baugh et al. and col. 9, lines 56-58 of Herlin et al.).

Regarding claims 10,20 and 30, the combination of Baugh et al. as modified by Herlin et al./Ashby et al. teaches further comprising the step of exchanging said private key between said computer system and said second computer system prior to transmitting said encrypted voice file (see col. 5, lines 31-33 of Herlin et al.).

#### **(10) Response to Argument**

Applicant argues the combination of references does not teach “providing a computer system coupled between a microphone and said radio, wherein inputs into said radio are received first by said computer system” (see page 12 of the appeal brief).

Regarding applicant's argument, examiner disagrees. Ashby shows a conventional radio with the microphone port and speaker port (figure 2 of Ashby). The applicant contends that Ashby does not show a computer placed in between the radio and the microphone, as shown by figure 2 of Ashby. However, claim 1 of the instant application is a method claim, and as such, has no structure. Therefore, referring to figure 4 of Ashby shows a process wherein a microphone outputs audio to a computing

device, which then outputs data into the radio. In that regard, the computer system IS coupled between a microphone and a radio.

As for claim 11, which is a system claim, the coupling of the microphone to the computer system leaves room for interpretation to be either a physical separation from the radio or a logical separation from the radio. Additionally, page 16, first full paragraph of the appeal brief, applicant argues that Ashby's radio is a conventional radio in the aspect of microphones being incorporated into the radio. The first limitation of claim 1 and 11 (the independent claims) specifically calls for a conventional radio remaining unmodified. If this is true, how can the conventional radio of Ashby not be conventional enough for the conventional radio in applicant's independent claims?

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Brandon Hoffman

*Brandon Hoffman*

Conferees:

Ben Lanier

*Ben Lanier*

Gilberto Barron

*Gilberto Barron*

*Gilberto Barron Jr*  
GILBERTO BARRÓN JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100